Аудит сетевой инфраструктуры

Модернизация информационной инфраструктуры обычно начинается с аудита, затем следуют выработка целей и плана ее развития, реализация которого восстанавливает необходимый уровень информационных технологий и делает дальнейшее развитие информационной инфраструктуры целенаправленным и управляемым процессом.

Периодический аудит информационной инфраструктуры дает представление о соответствии ее состояния.

Кроме того, аудит помогает оценить состояние отдельных элементов инфраструктуры и связанные с ними риски, а значит, позволяет определить, какие элементы информационной инфраструктуры должны совершенствоваться в первую очередь. К настоящему времени разработаны различные методики аудита информационной инфраструктуры.

Методики аудита

Крупные консалтинговые компании предлагают ИТ аудит, позволяющий оценить риски, связанные с информационной инфраструктурой: недостаточной надежностью, безопасностью или функциональностью информационной инфраструктуры в целом либо ее отдельных элементов

Системные интеграторы предлагают аудит, направленный на оценку качества сети, выявление проблем ее функционирования и выработку рекомендаций, обеспечивающих устранение этих проблем

Цели аудита сетевой инфраструктуры

- Выявление проблем функционирования ТИ и составление рекомендаций по их устранению.

Предоставление заказчику информации о выявленных проблемах с ТИ и рекомендаций по их устранению.

- Оценка качества ТИ.

Заказчику предоставляются данные о соответствии ТИ его деловым потребностям, решаемым задачам, стандартам (межгосударственным, национальным, международным и внутрикорпоративным), рекомендациям производителей оборудования и общим принципам создания аналогичных систем. Может быть оценена интегральная стоимость ТИ и совокупная стоимость владения.

- Инвентаризация и документирование ТИ.

Заказчик получает комплект эксплуатационной документации, облегчающей решение задач текущей эксплуатации (добавление и удаление пользователей, внедрение новых приложений и т. п.), а также поиск и устранение проблем

Порядок проведения аудита

Вне зависимости от объекта обследования проведение аудита включает три основных этапа:

1) постановка задачи и уточнение границ работ;

2) сбор данных;

3) анализ данных и оформление результатов

Постановка задачи и уточнение границ

- В ходе этого этапа выявляются элементы ТИ, подлежащие обследованию, такие как активное сетевое оборудование, кабельные системы, системы управления сетью и другие.
- Фиксируется их количество, расположение, определяется круг лиц, непосредственно эксплуатирующих ТИ, отвечающих за ее эксплуатацию и использующих ее в работе.

Сбор данных

На этом этапе обычно проводят интервьюирование персонала заказчика, осмотр и инвентаризацию оборудования, сбор конфигурационной и операционной информации, измерения различных параметров сети.

Сбор данных может включать следующие типовые работы:

- интервьюирование персонала заказчика;
- анализ представленных документов;
- приборные измерения;
- сбор конфигурационной и операционной информации;
- осмотр оборудования

Анализ данных и оформление результатов аудита

Эти работы также определяются ТЗ. При их выполнении проводится проверка собранных данных на полноту и корректность, анализ полученной информации, формирование выводов и рекомендаций, оформление и презентация результатов. В ходе анализа может быть принято решение о сборе дополнительных данных.

Этап анализа данных и оформления результатов обычно включает следующие типовые работы:

- проверка собранных данных;
- анализ структуры ТИ;
- анализ конфигурационных файлов;
- анализ операционного состояния ТИ;
- подготовка аналитического отчета;
- подготовка эксплуатационной документации;
- презентация результатов

Представление результатов аудита

Минимальный комплект эксплуатационной документации на ТИ обычно включает следующие документы:

- схему топологии сети;
- таблицу конфигурации сетевых устройств;
- таблицу конфигурации устройств, подключаемых к сети.

Более **полный комплект** предусматривает дополнительные документы:

- отдельные схемы топологии сети на канальном и сетевом уровне;
- инструкции обслуживающему персоналу;
- таблицы коммутации;
- профили пользователей;
- профили приложений.

Технические средства аудита

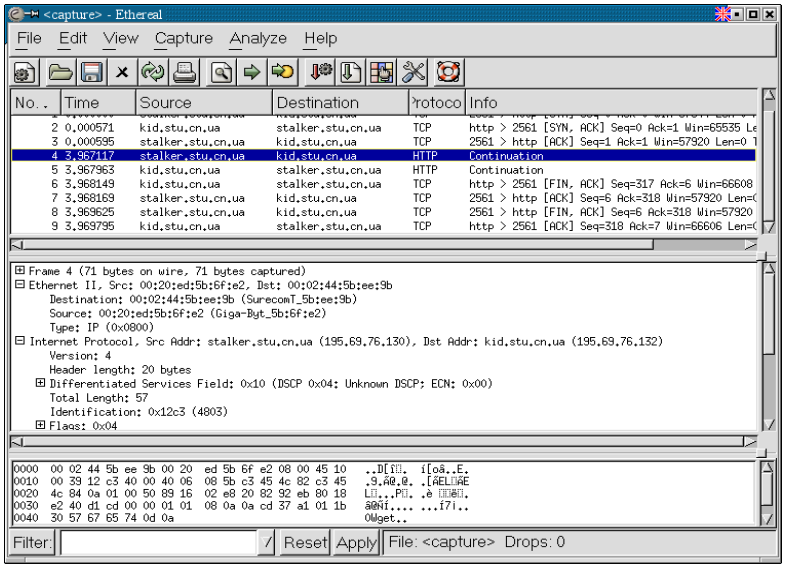
Используемые при аудите ТИ ряд технических средств, можно разбить на две группы.

В **первую** входят различные **анализаторы сетевого трафика:**

- **Аппаратный сетевой анализатор** Acterna DA 3400.

Позволяет анализировать множество сетевых протоколов на высокой скорости (Gigabit Ethernet), может имитировать загрузку сегментов сети, допускает подключение в разрыв сетевого кабеля.

- **Анализаторы Ethereal** (один из лучших бесплатных продуктов), **Observer** (коммерческий продукт). Устанавливаются на ПК, применяются, как правило, в связке со средствами захвата и отражения трафика (SPAN порты коммутаторов Cisco)



Вторая группа включает средства автоматизированного анализа сообщений об ошибках и анализа файлов журналов.

- Средство **Cisco Output Interpreter** обеспечивает автоматизированный поиск ошибок в конфигурациях, сообщений о проблемах в файлах журналов.

- **Анализатор Sawmill** обеспечивает анализ журналов одновременно из нескольких источников и позволяет находить корреляции между сообщениями об ошибках.